Paper Trail Manipulation III
Ronald E. Crane (voting@lastland.net)
11/28/2006

Taxonomy

Wholesale, paper-trail subversion.

Applicability

All systems using paper trails that voters do not manually deposit into a receipt box or ballot box.

Method

This attack immunizes Paper Trail Manipulation II (Shamos 2005)[1] from a certain audit.

Shamos describes Paper Trail Manipulation II ("II") thusly:

> …the system always produces accurate voter-verified ballots,[2] but when a voter votes for candidate A, then with probability p the ballot is voided by the machine even though the voter indicates assent, and no electronic record is made. After the voter leaves the machine, a new and non-voided ballot is printed with a vote for candidate B and an electronic record of this ballot is properly made. The second ballot is also deposited automatically in the ballot box. This effectively switches a vote from A to B.

Manipulation II can be detected by auditing the paper trail for a disproportionate number of cancellations (voids) of votes for candidate A followed by re-votes for candidate B.[3] Armed with sufficient baseline statistical information, one might be able to quantify and even to back out Manipulation II's effects.

Paper Trail Manipulation III incorporates II, but also generates dummy cancellations that disguise its election-skewing effect. When a voter votes for candidate A, then with probability p the machine first prints a paper trail containing a vote for candidate B, followed by a cancellation of that vote, followed by a properly-formed paper trail containing a vote for candidate A. The voter reviews the paper trail and accepts it, since it accurately records her selections. The machine then records an electronic record containing a vote for candidate A and deposits the paper trail into the collection box.

The machine does not apply both Manipulation II and Manipulation III to any one voter's ballot.

When the polls are closed, the attacking software removes all trace of itself so that post-election inspections (if any) reveal nothing unusual.

Resource requirements

The attacker must have the knowledge, ability, and access to conceive, develop, test, and deploy the attack. Employees of a voting system vendor are ideally placed to attack many jurisdictions' systems at once. Probably only a very small number of attackers need conspire to launch a successful attack.[4]

Potential gain

Massive and nationwide, depending on where the attack is deployed (e.g., at the vendor, at the state level, locally), the value of p, how many races the attacker targets, and how close the attacked races would be if not for the attack.

Likelihood of detection

Very low if the jurisdictions under attack do not conduct rigorous parallel testing. Some voters might observe that their machines seem to be printing a lot of information. An occasional voter

might glimpse a cancelled paper trail before it scrolls out of view,[5] and might, in consequence, question pollworkers, but this procedure is unlikely to precipitate even a local investigation.

The cancelled paper trails will appear entirely ordinary and the electronic and paper counts will match. An audit will reveal an excessive number of cancellations.[6] However, the number of cancellations of A followed by votes for B will approximately equal the number of cancellations of B followed by votes for A. Thus, auditors probably will assume that no attack has occurred, and that the cancellations resulted from voter error or from a candidate-neutral system "glitch."

An audit that compares cancellation rates between attacked and non-attacked precincts would suggest some kind of attack, but the machines would preserve no hard information of its nature. A more advanced attack would sidestep this audit by dividing precincts into those under active attack and those under a diversion-creating "passive" attack. The passive attack would create an approximately equal number of dummy cancellations from A to B and from B to A without actually shifting any votes.

Countermeasures

Preventive measures

This attack will not work with systems in which the voter physically deposits the paper trail (or a machine-printed paper ballot) in a collection box herself. In such systems the machine cannot void the original trail/ballot or print another.

Publicly-disclosed source code, citizen source vs. executable verification, and election-day citizen verification of the executables actually installed in the machines can deter some attacks, but attackers will then choose more subtle means (e.g., a Malware Loader[7]) to deploy their attacks.

The most effective preventive for this and other attacks is to refrain from using voting systems that place a computational intermediary between voters and their ballots. Thus, for example, hand-filled machine-counted (or hand-counted) paper ballots are not subject to this attack, nor to many others that affect computational intermediaries.

Detection measures:

See "likelihood of detection," above.

Retrospective:

"Voter-verified paper trails" are much less effective against attacks than is ordinarily assumed. They are truly voter-verified only if most voters check them[8] and if there is no opportunity for the voting machine to manipulate or to replace them afterward.

---

[1] http://vote.nist.gov/threats/papers/papertrailhack2.pdf (visited 11/28/2006).

[2] Shamos uses the term "ballot" here to mean the paper trail.

[3] The Brennan Center suggested a similar audit in its report "The Machinery of Democracy: Protecting Elections in an Electronic World" (hereafter "Brennan") at pp.70 and 87, http://brennancenter.org/dynamic/subpages/download_file_36343.pdf (visited 11/28/2006).

[4] The Brennan Center concluded that only one to three well-placed attackers successfully could carry out a software-based attack against VVPAT machines. Brennan at p.75. The Brennan attack involved deploying an attack program that falsified both the electronic records and the paper trails, and relied upon most voters not checking the paper trails and upon the absence of effective audits. Id. at 69-70. Since Manipulation III gives even careful voters (and auditors)

essentially no information that any fraud is taking place, it should be less amenable to detection than the Brennan attack, and should require no more conspirators to execute.

[5] Depending upon the machine's design, it might be able to print the cancelled paper trail and rapidly scroll it out of view before even an eagle-eyed voter could read it.

[6] Currently no state conducts audits of cancellations. Brennan at p.71.

[7] http://vote.nist.gov/threats/papers/malware_loader.pdf (visited 11/28/2006).

[8] Voters in a paper-trail test conducted by Selker and Cohen detected fewer than 3% of simulated errors. Brennan at p.66.